

WHAT IS CLAIMED IS:

1. A method for filtering out exploits passing through a device, comprising:
receiving an object directed to the device;
determining a first value associated with the object;
determining a second set of values associated with objects that have previously been scanned;
if the first value matches at least one of the values in the second set,
determining a third value associated with the object;
determining a fourth set of values associated with the objects that have previously been scanned; and
if the third value matches at least one of the values in the fourth set, immediately processing the object.
2. The method of Claim 1, wherein the object includes at least one of a message, an attachment to a message, an email, a computer-executable file, and a data file.
3. The method of claim 1, wherein the at least one of the first value and the third value further comprises at least one of a hash value, an algorithmic function, a checksum, a public key certificate, and a digital signature.
4. The method of Claim 1, wherein the first value includes a rough outline hash value (ROHV).
5. The method of Claim 4, wherein the third value includes a sophisticated signature hash value (SSHV) and wherein the ROHV requires less time to compute than the SSHV.
6. The method of Claim 1, wherein immediately processing the object further comprises processing the object without scanning the object.

7. The method of Claim 6, wherein immediately processing the object further comprises removing an exploit from the object.

8. The method of Claim 6, wherein immediately processing the object further comprises forwarding the object to a destination.

9. The method of Claim 1, further comprising if the first value does not match any of the values in the second set,
scanning the object for an exploit; and
updating the second set of values to include the first value.

10. The method of Claim 1, further comprising if the third value does not match any of the values in the fourth set,
scanning the object for an exploit; and
updating the fourth set of values to include the third value.

11. The method of claim 1, wherein the method is operable on at least one of a firewall, a router, a switch, a server, and a dedicated platform.

12. A computer-readable medium encoded with a data-structure, comprising:
a first indexing data field having indexing entries, each indexing entry including a first value; and
a second data field including object-related entries, each object-related entry having a second value and being indexed to an indexing entry in the first indexing data field, each object-related entry being uniquely associated with an object that has been previously scanned.

13. The computer-readable medium of Claim 12, wherein at least one of the first value and the second value further comprises at least one of a hash value, an algorithmic function, checksum, public key certificate, and a digital signature.

14. The computer-readable medium of Claim 12, wherein the first value is a ROHV.
15. The computer-readable medium of Claim 12, wherein the second value is a SSHV.
16. The computer-readable medium of Claim 12, wherein at least one object-related entry in the second data field includes information about the associated object.
17. A system for protecting a device against an exploit, comprising:
a message tracker that is configured to determine whether an object has been previously scanned using a two-phase hash value technique; and
a scanner component that is coupled to the message tracker and that is configured to receive an unscanned object and to determine whether the unscanned object includes an exploit.
18. The system of Claim 17, wherein the object includes at least one of a message, an attachment to a message, an email, a computer-executable file, and a data file.
19. The system of Claim 17, wherein the two-phase hash value technique comprises:
determining a first value associated with the object;
determining a second set of values associated with objects that have previously been scanned; and
if the first value does not match at least one of the values in the second set, determining that the object has not been previously scanned.
20. The system of Claim 19, wherein the first value further comprises at least one of a hash value, an algorithmic function, checksum, public key certificate, and a digital signature.

21. The system of Claim 19, wherein the first value further comprises a ROHV.
22. The system of claim 19, wherein the two-phase hash value technique further comprises:
if the first value matches at least one of the values in the second set,
determining a third value associated with the object;
determining a fourth set of values associated with the objects that have previously been scanned;
if the third value does not match at least one of the values in the fourth set, determining that the object has not been previously scanned.
23. The system of Claim 22, wherein the third value further comprises at least one of a hash value, an algorithmic function, checksum, public key certificate, and a digital signature.
24. The system of Claim 22, wherein the third value further comprises a SSHV.
25. The system of Claim 22, wherein the two-phase hash value technique further comprises:
if the third value approximately matches at least one of the values in the fourth set, determining that the object has been previously scanned.
26. The system of Claim 17, wherein the system is operable on at least one of a firewall, a router, a switch, a server, and a dedicated platform.
27. An apparatus for protecting a device against an exploit, comprising:
means for receiving an object directed to the device;
means for determining whether the object has been previously scanned using a two-phase hash value technique; and

means for immediately processing the object if the object has been previously scanned.

28. The apparatus of Claim 27, further comprising means for scanning the object if the object has not been previously scanned.

29. The apparatus of Claim 27, further comprising:
means for maintaining a list of previously scanned objects for the two-phase hash value technique; and
means for updating the list.